(19) Europäisches Patentamt
European Patent Offic
Offic urop´ n d s br v ts

(11) EP 0 998 091 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
03.05.2000 Bulletin 2000/18

(51) Int. Cl.⁷: **H04L 29/06**, H04L 12/22

(21) Application number: **99116343.7**

(22) Date of filing: **19.08.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.08.1998 US 136682**

(71) Applicant: **PLATINUM TECHNOLOGY IP, INC.**
Oakbrook Terrace, IL 60181-5241 (US)

(72) Inventors:
, Creighton Broadhurst, Christopher John
Farley Hill Reading RG 1 1UU (GB)
, Byrne, Barry Anthony
Wokingham RG41 4LJ (GB)
, White, Clive John
Berks RG41 3AL (GB)
, Press, James
Bedfordshire, SG 18 OHP (GB)
, McMahon, Piers
Westlea, SN5 7EH (GB)

(74) Representative:
Patentanwälte
Gesthuysen, von Rohr, Weidener, Häckel
Postfach 10 13 54
45013 Essen (DE)

(54) System and method for web server user authentication

(57) A method and a system for automatically authenticating a user to applications in a network environment are proposed. After an initial authentication procedure, the user's identity is mapped into a network credential which includes the user's role, and which is formed into a cookie. To gain access to an application requiring authentication, the cookie is provided to a script, and the information contained in the cookie is used to obtain authentication data required by the desired application.

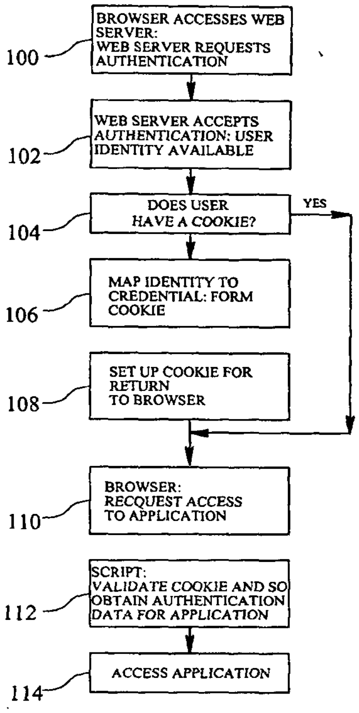
BROWSER ACCESSES WEB SERVER: WEB SERVER REQUESTS AUTHENTICATION
100
WEB SERVER ACCEPTS AUTHENTICATION: USER IDENTITY AVAILABLE
102
DOES USER HAVE A COOKIE?
YES
104
MAP IDENTITY TO CREDENTIAL: FORM COOKIE
106
SET UP COOKIE FOR RETURN TO BROWSER
108
BROWSER: RECQUEST ACCESS TO APPLICATION
110
SCRIPT: VALIDATE COOKIE AND SO OBTAIN AUTHENTICATION DATA FOR APPLICATION
112
ACCESS APPLICATION
114

Fig. 2

Description

[0001] The present invention relates generally to networked computer systems. More particularly, the present invention relates to user authentication and access to back-end or external applications via a web server. In particular, the present invention relates to a method for accessing resources on a network and to a system for providing user access to web server resources.

[0002] In a typical web-based server application, user access to information is achieved via a web server, with the application requiring the user to be authenticated by, e.g., a user id and/or a password. When a user desires access to a new application (such as a database management system (DBMS) engine; new applications will often have a different configuration and/or manufacturer than the initial application), such a new server has a login/authentication procedure which is independent of previous login/authentication procedures encountered by the user. To access the web pages, appropriate identification credentials must be presented to the new application. This is conventionally accomplished by requiring the user to input additional login/authentication information specific to the new application, or by hard-coding a generic login and password in the scripts used by the user's web server to access the new application and dynamically generate a new web page using the output from the application.

[0003] Both of these solutions are unsatisfactory. Requiring the user to input additional information places a burden on the user to remember multiple logins and passwords, further places a burden on each server and system administrator to maintain multiple user accounts for each and every access by a user, and is a potential security risk because passwords are transmitted unencrypted over the network. Using a generic or static login and password in a script is a potential security hole and does not readily provide different levels of access based on the identity of the user.

[0004] These issues have been addressed by the so-called new technology LAN manager (NTLM) automated authentication system. In the NTLM system, once the user is initially authenticated to a Microsoft network or to a Microsoft Windows NT domain (using a password), similar components (the web browser and server) can assure one another of the user's identity. This assurance occurs transparently to the user. However, this system does not perform authentication to a new application (beyond the server). Thus, the NTLM authentication system is of limited utility for many users.

[0005] U.S. Patent 5,689,638 discloses a method and system for accessing independent network resources without prompting the user for authentication data. When the system receives a user request to access an independent network resource, system logon and server authentication data is autonomously supplied to the independent network resource without further user interaction. U.S. Patent 5,689,638, however, is not concerned with a world-wide web hypertext transfer protocol environment, and is not concerned with authentication information based on the user's role. In the system according to U.S. Patent 5,689,638, a password cache is maintained in the main memory of a local computer system. The password cache contains a server name, user name and password for each server to be accessed by a particular user. When presented with an access request, network software searches the password cache structure for the server authentication information before passing it on to the server to be accessed.

[0006] U.S. Patent 5,678,041 discloses a system and method that restricts a user's access of Internet information based on a rating category and/or ID associated with a particular terminal through the implementation of a firewall internal to a user's computer network. The firewall prevents the user from accessing certain types of Internet information (e.g., prevents children from accessing obscene material, prevents workers from accessing non-work related material, etc.). Thus, U.S. Patent 5,678,041 is concerned with an internal authorization to access remote resources (which are presumed to be public resources), and is not concerned with a system in which authentication information is required by the remote resources.

[0007] It would be desirable to allow a user to easily, automatically, and transparently authorized to access, via a web server, a plurality of applications which require authentication, whether in an intranet or internet environment. It would further be desirable for such a scheme to be implemented in a hypertext transfer protocol (HTTP) environment, and to maintain the security of the network. It would further be desirable to allow access regardless of whether the applications are operating in the same or different environments.

[0008] It is an object of the present invention to provide an improved method for accessing resources on a network and an improved system for providing user access to web server resources, preferably achieving the advantages mentioned above.

[0009] The above object is achieved by a method for accessing resources on a network according to claim 1 and by a system for providing user access to web server resources according to claim 7. Preferred embodiments are subject of the subclaims.

[0010] In particular, the present invention overcomes the above-described problems, and achieves additional advantages, by providing for a system and method for authenticating a user in a web server environment, by providing for an authentication scheme in which users are logged in and authenticated a single time, yet can access multiple applications via a web server. According to exemplary embodiments, an initial authentication is performed to access a first application via a first server, and the user's identity is mapped into a network credential which includes a user role. Additional applications are accessed by providing the network credential to a script, retrieving script access values for the additional applications based on the network credential and presenting the script access values (as, for example, user name and password) to the additional applications.

[0011] The authentication scheme according to the present invention allows a user to access numerous protected resources with a single authentication procedure, greatly improving the user's ease of system use. Further, the use of role-based authentication simplifies system administration burdens. The present invention is particularly advantageous in an intranet environment.

[0012] The present invention will be more completely understood upon reading the following detailed description of exemplary embodiments in conjunction with the accompanying drawings, in which like reference indicia designate like elements. It shows:

FIG. 1 a block diagram of an intranet network in which the present invention can be implemented; and

FIG. 2 a flow chart describing a method of automatically authenticating a user to back end applications in a network according to the present invention.

[0013] Referring now to FIG. 1, a computer network suitable for the method and system of the present invention is shown. The network includes a plurality of computer workstations 10 and a plurality of servers 12 residing on host machine 13. Each workstation 10 includes a web browser 14 which serves as a user interface to allow the user to access resources in the network. Each server 12 acts as a gateway to provide the user access to various resources, including static HTML (web) pages 18, back-end applications 20 (e.g., a database management system running on the same machine as the web server) and external applications 22 (which run on a different machine than the web server). Access to the back end or external applications is provided through a script or application 17. Each server 12 is configured to allow access by a user to the server resources only upon user authentication to the server. The network also includes an X.500 or other suitable directory 16, which is a network wide data storage resource. More details about X.500 directories are contained in document ITU-T Rec.X.500 (1993) "Information Technology-Open Systems Interconnection - The Directory: Overview of Concepts, Models and Services."

[0014] To login to the network, an initial user authentication is performed, such as by a user inputting authentication information into one of the computer workstations 10. According to an aspect of the present invention, the initial authentication information is mapped to a role of the user. Examples of roles can include, but are not limited to, "executive", "clerk", "accounting" etc. Roles can be related to particular departments of an organization, with special designations for department heads. It is assumed that the number of potential user roles will be less than the number of potential users of the network. The user's role determines which applications, and hence which network resources, can be accessed by that user. For purposes of explanation, it is assumed that the network of FIG. 1 is part of an intranet. As will be appreciated by those of ordinary skill in the art, an intranet is a network which uses the same types of software and components as the Internet, but the intranet is reserved for private use only. It is increasingly common for private entities to have web servers which are accessible only to certain persons. While the discussion assumes an intranet environment, it will of course be appreciated that the principles of the present invention can be readily adapted for use in other network environments.

[0015] For each user, the directory 14 stores information which allows the user's authentication information to be mapped into a network credential which includes a role of the user. The network credential can then be formed into a cookie. Once logged in and initially authenticated to the network, a user may freely access any of the applications allowed by the role.

[0016] To access additional resources not included in the initial list, the user inputs a request to access additional resources, which may be associated with the user's initial server or a new server in the network. Access to the back end or external application is achieved using a script (a series of commands which can be executed without user interaction) or other similar means accessible as a web server resource. The script is written by the system administrator, stored on the same host machine as the web server, and provides the login code for the server/application. The user name and password are not hardcoded into the script, but rather are stored in script access procedure variables (SV) having names chosen by the system administrator. The password values are preferably encrypted to enhance security. The SV's are stored in a database which can be the directory 16 or another suitable database (such as database 19 associated with the server host 13) accessible to the server. According to an aspect of the present invention, in response to a user request through the browser, the script retrieves the SV value from the directory 16 based on an SV name contained in the script, the user's role and identity (contained in a cookie provided to the script). In this manner, the identity and password used by the user to access the third party application are determined by the user's role and individual identity.

[0017] Referring now to FIG. 2, a flow chart describing an exemplary method according to the present invention is shown. The method begins in step 100, where a user logs on to the network (e.g., the network shown in FIG. 1) using any conventional login procedure, and the browser accesses a web server. In step 102, an initial authentication procedure is performed, and is accepted by the server to establish a user identity to the server. The initial authentication can be achieved using basic authentication (which requires user interaction), NTLM (which requires no user interaction), X.509 certificate (which may or may not require user interaction), or other suitable means. More details about X.509 certificates are provided in document ITU-T Rec.X.509 (1993), entitled "Information Technology - Open Systems Interconnection: The Directory: Authentication Framework." In step 104, it is determined whether the user already has a cookie containing a network credential. If there is not yet a user cookie, one is created in step 106 by consulting the directory 16 to map the user's identity to an intermediate identity and a user role, which are used to form a network credential. If no mapping can be found between the user's local identity and a network credential, a "no-map" cookie is created to prevent repeated failed lookups. The user's network credential, including user role, is formed into a cookie by appending the identity of the user's terminal to the credential, and making a cryptographic seal of the result. The cookie is then preferably encoded. As will be appreciated by those of ordinary skill in the art, a cookie is a message given to a web browser by a web server to record aspects of the interaction history between the browser and server, and which is stored by the web browser to facilitate access to additional server resources. The cookie is preferably configured to disappear when the browser program is closed by the user. In step 108, the cookie is returned to the browser.

[0018] Note that if there is already a cookie for the user, the process skips steps 106 and 108, and proceeds to step 110.

[0019] In step 110, the user attempts access to a new application (a back-end application resident on the same host machine as the web server or an external application not resident on the same host machine as the web server) by inputting a request to the browser, which then attempts to access the requested resources. These additional resources may or may not be accessible to the user based on the user's assigned role. In step 112, the browser obtains authentication information, in the form of SV values necessary to access the back-end or external application, by accessing a script for single sign on stored with the web server, and transferring the cookie to the script. The script retrieves the script access variable for the back-end or external application based on the network credential (including the user role), and presents the SV values to the new application. Step 112 is performed automatically by the browser without any action required on the part of the user beyond presenting the request in step 108. In step 114, the desired application grants access based on the authentication information obtained in step 112.

[0020] While the foregoing description includes many details and specificities, these are included only for purposes of illustration, and are not intended to limit the invention. Many modifications to the examples described above will be readily apparent to those of ordinary skill in the art which do not depart from the scope of the invention, as defined by the following claims and their legal equivalents.

[0021] The roles can also be understood as a means for classifying the users and can preferably include respective classification parameters. Further, a cookie can also have the form of a small program, a program part, or a set of parameters.

Claims

1. Method for accessing resources on a network, comprising the steps of:

    performing an initial authentication of a user via a web server;

    creating a network credential for the authenticated user, the network credential including at least a role of the user; and

    providing secondary access to one or more applications via the web server by receiving a user request, automatically accessing a script, transferring the network credential to the script, retrieving script access values for the one or more applications based on the network credential, and presenting the script access values to the one or more applications.

2. Method according to claim 1, characterized in that the number of roles is less than the number of network users.

3. Method according to claim 1 or 2, characterized in that the method further comprises the step of forming a cookie from the network credential.

4. Method according to claim 3, characterized in that the step of transferring the network credential is performed by transferring the cookie.

5. Method according to any one of the preceding claims, characterized in that the step of creating is performed by mapping user initial authentication data to the network credential by consulting an X.500 directory.

6. Method according to any one of the preceding claims, characterized in that the network is an intranet.

7. System for providing user access to web server resources, comprising:

    a plurality of servers (12) for managing network resources, each server (12) configured to grant access only upon user authentication;

    a browser (14) communicating between the user and the plurality of servers (12), the browser (14) being capable of accessing initial user authentication information; and

    a directory (16) for storing data defining mappings between initial user authentication data and network credentials, the network credentials including at least a user role;

    wherein the browser (14) provides user access to protected applications (18, 20, 22) via a web server (12) based on the initial authentication information, and by consulting the directory (16) transparently to the user.

8. System according to claim 7, characterized in that the servers (12) are intranet network servers.

9. System according to claim 7 or 8, characterized in that the number of user roles is less than the number of

system users.

10. System according to any one of claims 7 to 9, characterized in that the browser (14) communicates with the servers (12) according to a hypertext transfer protocol format.

11. System according to any one of claims 7 to 10, characterized in that the first server (12) creates a cookie including the user role, and the browser (14) provides access to the second application by providing the cookie to a script which is stored on the network.

12. System according to claim 11, characterized in that the first server (12) accesses script access values stored in a database for the second application based on the cookie.

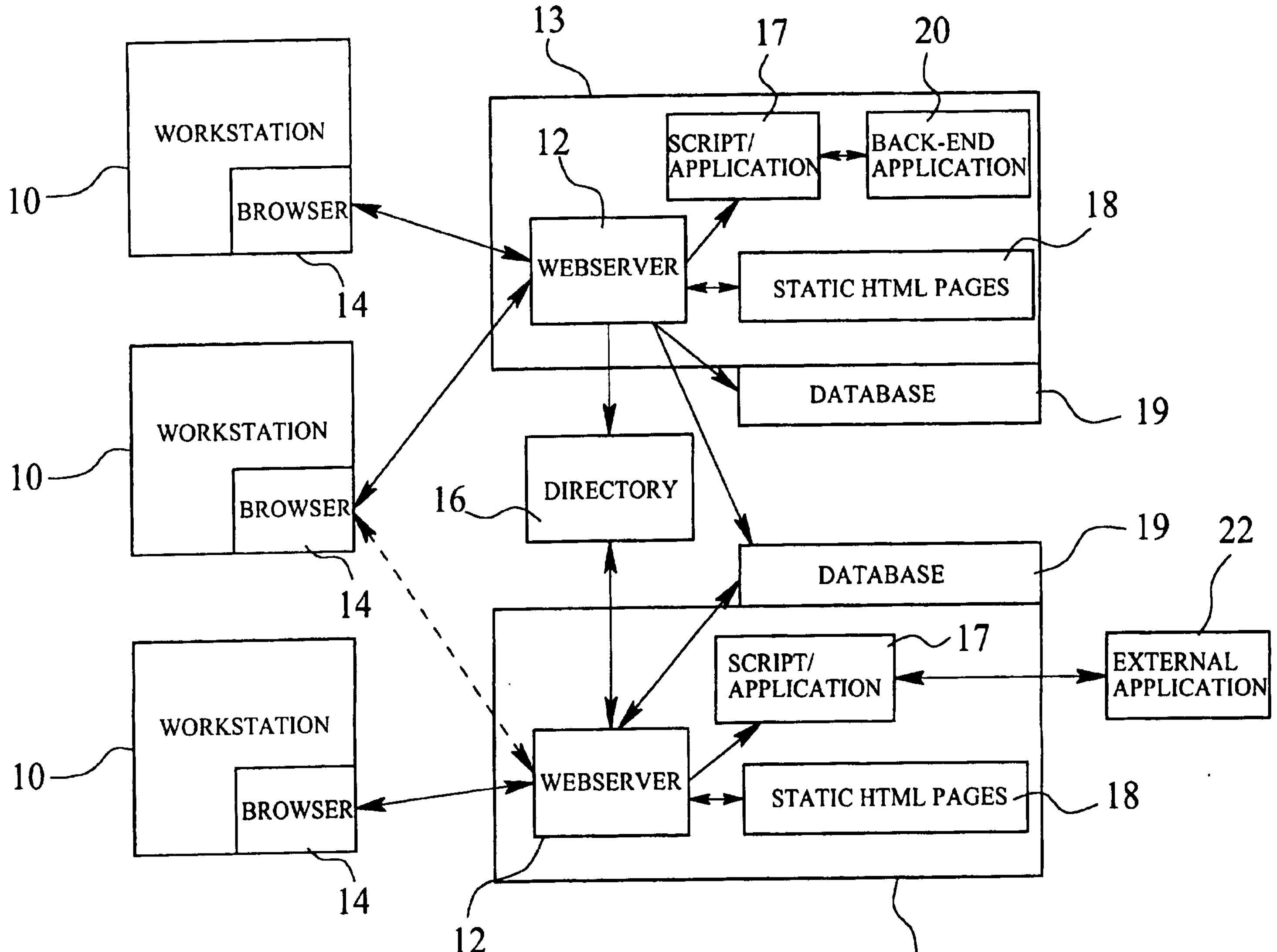
13
17
20
12
SCRIPT/
APPLICATION
BACK-END
APPLICATION
18
WORKSTATION
10
BROWSER
WEBSERVER
STATIC HTML PAGES
14
DATABASE
19
WORKSTATION
10
DIRECTORY
16
BROWSER
14
19
22
DATABASE
17
SCRIPT/
APPLICATION
EXTERNAL
APPLICATION
WORKSTATION
10
WEBSERVER
STATIC HTML PAGES
18
BROWSER
14
12
13

Fig. 1

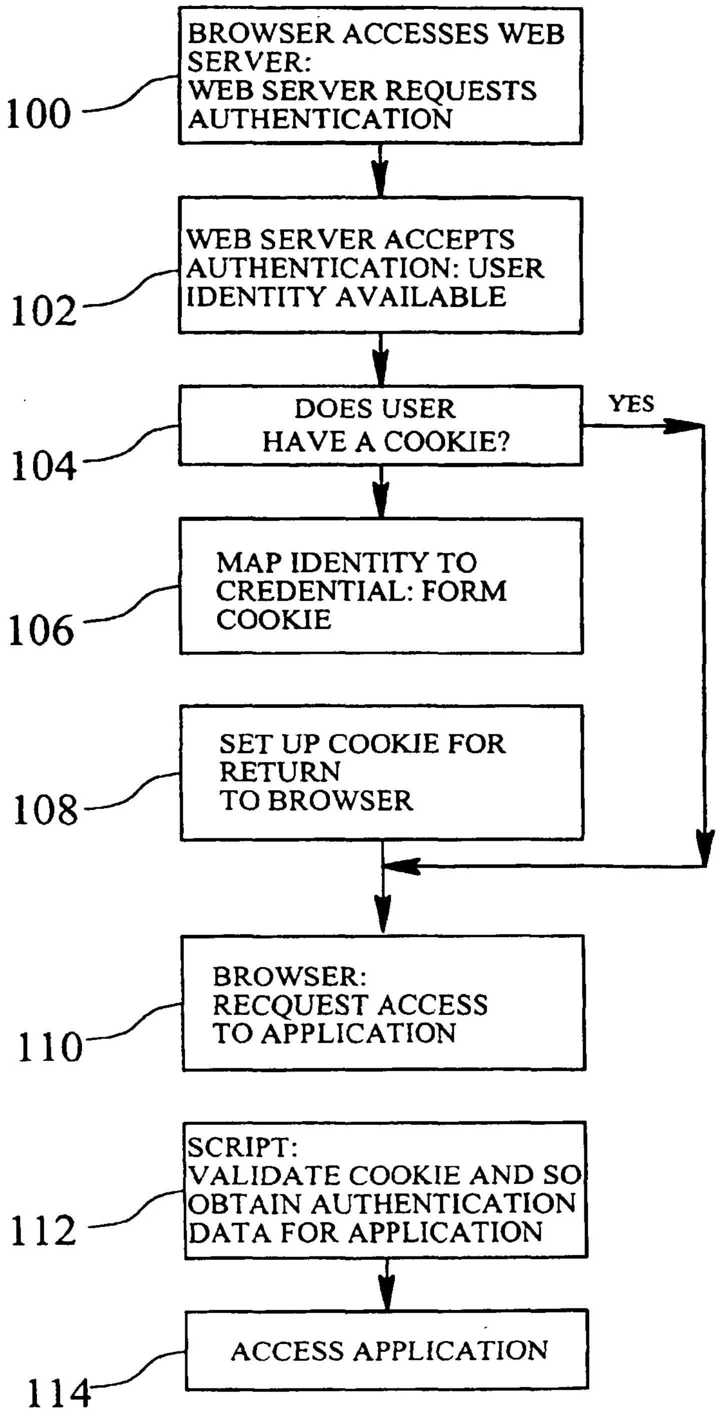
BROWSER ACCESSES WEB SERVER:
WEB SERVER REQUESTS AUTHENTICATION
100
WEB SERVER ACCEPTS AUTHENTICATION: USER IDENTITY AVAILABLE
102
DOES USER HAVE A COOKIE?
YES
104
MAP IDENTITY TO CREDENTIAL: FORM COOKIE
106
SET UP COOKIE FOR RETURN TO BROWSER
108
BROWSER:
RECQUEST ACCESS TO APPLICATION
110
SCRIPT:
VALIDATE COOKIE AND SO OBTAIN AUTHENTICATION DATA FOR APPLICATION
112
ACCESS APPLICATION
114

Fig. 2